PCT/DK03/00016

Kongeriget Danmark

Patent application No.:	PA 2002 00036
Date of filing:	10 January 2002
Applicant:	Neupart ApS Vesterbrogade 149 1620 København V

This is to certify the correctness of the following information:

The attached document is a true copy of the following document:

- The specification, claims, abstract and drawings as filed with the application on the filing date indicated above.

Patent- og Varemærkestyrelsen
Økonomi- og Erhvervsministeriet

11 February 2003

D. Søndergaard
Dorthe Søndergaard
Information Specialist

Information Security Awareness system

Summary of the invention

The invention is a method and computer software that on a modular platform provides security policy management, security survey, and security education to individuals in organisations. The three elements are used all together or separately. By utilising the invention users gain increased security awareness, increased knowledge and ability to impact their actions in a security cautious way. Organisations, e.g. businesses or companies, gain increased information security, increased return of investment in existing security technologies and products and reduced risk of costly security incidents.

The software runs in two different set-up's: 1) in a hosted environment in order to provide the defined functions and services. 2) Stand-alone execution that in addition to the hosted environment also runs on servers at business users or business partners in order to provide the defined functions and services.

The computer software can execute on a standard business style networked computer, for example a server type computer with hard drives, computing power, memory and input/output devices or the software can execute on a dedicated computer device with storage capacity, computing power, memory and input/output devices

The invention is implemented using software running on computers. The software contains user interface modules for each of the modules, business logic, an information security object database as well as interfaces between the users and the modules and interfaces in between the modules.

Description

User interface

User interface to policy, survey, education and management modules.

The invention provides full functionality to users through an Internet browser, e.g. MS Internet Explorer, Netscape, Mozilla, or Opera.

Email messages can be used to direct users to the appropriate network address that can be accessed by an Internet Browser.

User interface to the modules can optionally be implemented using stand-alone applications (versus browser based).

Language

The invention is supporting multiple languages both in terms of the software itself and in terms of the content elements, e.g. the information security objects, that is managed by the invention.

Policy module

This module is a tool for security policy management. Users of the module use the Policy module to generate and manage a set of easy to use security policies. The content in these policies will be re-used in the survey module and in the education module.

Definitions

A policy is a number of records in the policy table in the Information Security Object database (ISO-DB). The records relate to a specific customer organisation and contain the following content.

Customer	Object Category	Information security object	Object Content

Customers is an identifier that links to a separate customer table that optionally links to a CRM system. The operator (or superuser) creates a customer in the customer table of the database after receiving an order or after agreeing to a demonstration for a specific client.

Object Categories identifies the type of information security object to which the record relates. It contains text. E.g. does the information security object impact "computer user behaviour", does it impact only the "IT-department", or is it about "physical access". There will typically be a number of Information security objects with the same category. Example: More than one information security object is to regulate the physical access to the customer's information assets.

Information security object descriptor is the object description itself; it contains a text string or a link to a text string that describes the object. Examples include: "Passwords are required to contain a variety of different character types." and "Passwords are required to have a minimum length". Objects are unique within the customer's policy, and the Manager selects the information security object from lists of object templates that content providers define. These lists are stored in tables for Information security object templates. Objects that are not already in the policy are may be marked e.g. "Unused", or "New", or Customer specific".

Object Content holds the content or the value of the Information security object. The value is a text string. The Manager can choose the content from a list where all entries relate to the Information security object. Example: If the Information security object specifies that a certain password length is required, the object content field contains the exact value, e.g. "eight characters" and the list contains a number of other content that in some cases are acceptable. In the list, a field named "default security rating" indicates which Object Content options content providers consider the more secure choices.

Security Policy creation processes

A superuser ads name of organisation into the information security object database (ISO-DB).

- Either Default security policy is created:
- Superuser specifies the "default Security level profile" of the organisation.
- The system queries all information security objects (ISO) that matches the default security level profile and adds the result to the information security policy for the organisation, hereby generating an default current security policy.

Or, the ISO's are created based on existing text format security policies, security instructions, or security procedures.

Security Policy management processes

The default security policy is subsequent managed by a management user:
Information Security Objects can be added, edited or deleted.
Those ISO's that are not included in the current security policy are listed as e.g. unused objects, making it easy for the management user to see, monitor and review which ISO's that are deliberately not used in the current policy.
Unused ISO's can be made current by a simple selection.
New ISO's – e.g. organisational-specific objects - can be added to customer's current policy by the management user entering the required content, e.g. category, descriptor and value.

New default ISO's are added as the outcome of information security research performed by content providers.

Policy publication and communication.

The policies (or the security instructions, procedures etc) can be published, distributed or communicated to the end users through email, web servers (e.g. Internet, extranet or intranet sites) and not at least through the survey module and the education module.

Users, functions and user permissions.

The users of the policy module are by default and unless else is defined the same throughout all modules.

- Managers, who will typically be customer's security manager or security officer or consultant or a content provider who provides a manual policy service to the customer.
- Superusers, who may be content providers.
- Users, who will be computer users in the organisations of the customer.

The following table shows an example of user permissions:

User group:	*Users*	*Managers*	*Superusers*
Function:			
Read policy	✓	✓	✓
Add policy		✓	✓
Modify policy		✓	✓
Delete policy		✓	✓
Read information security objects	✓	✓	✓
Add information security objects		✓	✓
Modify information security objects		✓	✓
Delete information security objects		✓	✓
Read object content	✓	✓	✓
Add object content		✓	✓
Modify object content		✓	✓
Delete object content		✓	✓
Read object content templates		✓	✓
Add custom object content templates			✓
Modify custom content templates			✓
Delete content templates			✓
Acknowledge policy read and understood	✓		
Add Comment to Information security object and object content	✓		
Add, invite and delete users		✓	✓
Add, invite and delete managers			✓

Read survey content	✓	✓	✓
Add custom survey content		✓	✓
Modify custom content templates		✓	✓
Delete content templates			✓
Initiate surveys		✓	✓
Answer surveys	✓		
Read survey reports		✓	✓
Edit survey reports			✓
[illegible]			
Read and participate in learning sessions	✓	✓	✓
Update lessons		✓	✓

Display warning when user is trying to modify information security objects and object values that are already used in policies and have been read by users. Warning should suggest to consider adding a new object and value instead.

Information security objects and Object Contents are versioned and time stamped at last modification.

For Policy users, yet unread information security objects and object contents are marked "New".

Survey module

Process

The survey module invites users at specified intervals – default is every quarter of a year – to answer a questionnaire about general security knowledge and security policy specific knowledge.

Invitation e-mails are sent to users directly from the module to invited users or to customer's administrator. Emails contain a direct link (URL) to an online questionnaire that relates to the customer and contains sufficient access information for the user to gain access to the questionnaire. The content of the invitation email is customisable and with a default content provided.

The authentication of the survey users is based upon user's ability to receive an email at the specified email, or by digital certificates.

Users will be presented with a short privacy policy description with a link to a wording that comfortingly and clearly describes what user data are stored and how the results of the survey will be used and by whom.

Users can choose to respond anonymously resulting in that no personal information is stored, but the answers of the user will consolidate in the survey results. This feature provides that the manager chose to allow anonymous answers. Users choosing the anonymous option will be informed that questions might be repeated in later surveys and education.

The Survey system logs which users have answered, and a reminder process is initiated for those who did not participate before a deadline specified by the Manager. Default reminder is 7 days after first invitation email. Users are associated with minimum two group descriptions to enable grouped reporting and targeted, efficient follow up education.

Users can be provided with their score and the right answers immediately. Administrator receives a report by email that documents the responses and provides summary to make it easy to identify weak points in security chain and to educate efficiently in the right places.

The Survey is repeated quarterly or as requested by the organisation. The repetition allows to document the security level development and to add new components to policy or to awareness program as recommended by Neupart's threat research.

Reports

The module can generate survey result reports that are easy to read for people without security knowledge in e.g. executive staff or management as well as for security officers and managers. The reports contains graphically presented survey results documenting minimum the following items:

- Total knowledge score for company compared to average of all Survey respondents.

- Total knowledge score for company compared to average in same business vertical.
- Historical development in knowledge score with each previous survey results plotted along a time axis.
- Total knowledge score grouped by department.
- Total knowledge score grouped by Policy Categories.
- Department knowledge score grouped by Object Category.
- Historical development grouped by department.

The module also generates a report so that individual Users can see their own – hopefully for the users motivating ☺ - personal security score development chart.

The Survey module has the ability to ask more than one question per information security objects and object contents.

The module supports PGP encrypted emails to administrator, by allowing administrator to upload public PGP Key.

Education module

The lessons contained in the education module are presented to the users with E-learning lessons in the education module are using content from the central security object database.

The lessons that by default are offered to the user depends on the results from the survey module and upon which ISO categories the Manager has chosen to activate for the customer organisation to which the user belongs.

The user and the Manager have the option to select and de-select other modules than offered by default.

E-learning lessons or modules exist for each ISO category and for many types of Information security objects.

An e-learning lesson lasts 20 – 30 minutes to complete for an average user. This estimate is subject to educational expert advice.

The lessons are able to communicate both the generic information security content and content of the security policies in a motivating, appealing and catching way.

Database module

This module contains the core data structures of the invention.

These are implemented on a database platform that

- Can be distributed as full runtime versions to deliver a "in a box" type solutions-.
- Gives a high level of platform in-dependencies in order to solve high security requirements.

Management module

Contains

- Common user management routines for the three modules
- User access and authentication modules.
- All data maintenance routines and interfaces.

Admin's are authenticated at a higher level than end users, in order to meet the requirements of easy access to end users and high security in the system.

Features

Generic computer based Information Security learning to users

Using e-learning systems – online and offline - to provide information security lessons with generic content to all - or to groups of - computer users throughout any organisation.

Effects: Users gain better understanding of general information security aspects and can operate their work place computer with increased information security as a result.

Organisation-specific computer based Information Security learning

Using e-learning systems – online and offline - to provide information security lessons with organisation-specific content to all - or to groups of - computer users throughout any organisation.

Effects: Users gain better understanding of the security policies, descriptions, procedures and requirements in the organisation of which they are a member. Users can process and work with organisation's information security assets, e.g. documents, data, general information security aspects in an increased secure way, compared to if users have not obtained this understanding through the invention.

Multimedia based Information security learning

Using multimedia, e.g. sound, speak, voices, animations, moving pictures, video recordings and recorded computer screen shots to provide information security learning to computer users throughout the organisation.
Effects: Users become increasingly motivated to learn information security and to return to the learning process for further increased learning.

Generic Information security content in computer based user surveys

Having general Information security content and questions in electronically performed computer user surveys.
Effect: Survey participants become increasingly aware of the content in the survey. A survey report can be generated. A survey report can document the information security awareness among the computer users in the organisation. The survey results can also be used to target succeeding education more efficiently. The targeting can be done by groups of the organisation, or by individual.

Organisational-specific Information security content in computer based user surveys

Having individual (for an organisational) Information security content and questions in electronically performed computer user surveys.
Effects: Survey participants become increasingly aware of the organisational-specific content in the survey. A survey report can be generated. A survey report can document the specific knowledge about the information security awareness among the computer users in the organisation. The survey results can also be used to target succeeding education more efficiently. The targeting can be done by groups of the organisation, or by individual.

Targeting computer users throughout the organisation

Providing information security awareness, security lessons and security surveys targeted to computer users throughout the organisation.

Effects: The weakest link in the information security link is strengthened by the invention. The information security link consists of technology/products/systems as well as end user behaviour. End users without sufficient knowledge are the weakest link, and when strengthened through the invention, end users can choose a secure behaviour when working and when using computers to process information assets.

Storing information security policy in a database in the form of information security objects

Information security policies, Information security procedures, Information security instructions or, Information security rules are saved in a relational database. These document types are modularised and saved in a database as information security objects (ISO's) The objects contain, for example, specific or general information security objects and appropriate content or values of such objects.

Example: Assume a traditional style security policy specifies user' behaviour to be using password(s) with a certain minimum length, and assume that length is e.g. 6 characters long. In the relational database one record would be added with minimum the following *information security object* content:

1) *category is "user behaviour",*
2) *descriptor is "passwords with a certain minimum length are required to be used" and*
3) *the actual length that is required.*

Example 2: Assume a traditional style security policy stipulates rules for how users shall treat information assets. On area of regulations is about employees having papers and documents on the desktops. Users are required to clean their desktop for confidential papers by the end of each working day. In the relational database one record would be added with minimum the following information security object content:

1) *category is "information asset handling",*
2) *"rules for cleaning employees desktop for information, e.g. documents and papers"*

3) Employees must clean their desktop by the end of each working day.

Effect: Database based security policies, security procedures, security instructions, or security rules can be created, managed and be in other contexts with less manual efforts compared to traditional security policies and traditional policy management tools. The increased effectiveness also has the effect of increased information security to organisations and to users as security policies, security procedures, security instructions, or security rules are foundations for improved information security in organisations of any type.

Using information security objects in information security policies

The ISO's are stored in a database and are used as modular content for e.g. Information security policies, Information security procedures, Information security instructions, and Information security rules. The ISO's are assigned an unique identifier allowing organisations that create and maintain e.g. security policies to link to the identifier. The ISO's are also assigned values for "default security level value" are stored. The ISO's are also assigned a status value for each organisation.

Effects: Increased re-use of ISO's, as multiple organisations can choose and select without "re-writing" default ISO's to go into their policies.

By specifying a default security level value for a specific organisation, the invention makes is possible to automatically create a default policy, simply by querying the default ISO's that match the default security level value of the organisation.

The status value for each ISO makes it possible for an management user of an organisation to define values that sets the status. For example, ISO's with value "new since last" or "ready for review" can be processed and can be assigned a new status e.g. "Current" meaning it now is a part of the current policy. Similarly the status values can also have the effect of identifying which ISO's deliberately are not included in a policy, e.g. with the value "Unused". The status value also makes it possible to add custom content in an organisation's policies, since e.g. the value "Custom" can be used as such.

Using information security objects in information security surveys

The content of the information security objects are utilised for automatically generating relevant content of information security surveys. The ISO's that are also content in security policies are utilised for surveying e.g. user conformance, understanding, knowledge and awareness of the defined and current security policies and of information security aspects more general.

Effects: The surveys are generated much more effortless by re-using ISO's than by using traditional survey content and preparation methods.
The surveys contain more accurate and relevant content for the user.
Organisations using this invention gain more accurate reporting on topics of relevance and improved information security.

Example Content in survey

The organisational specific parts of the survey are queried in the information security object database.

Question	*Answer options*	*Right Answer*	*Comment*
Does you company have a set of security policies?	Yes/No	As defined in ISO-DB	
How aware are you about the content of the policies?	Fully/well/some/ not at all	Not defined	
According to your knowledge, does your company have policies about "<Policy Category>"	Yes/No/Don't know	Yes if <Policy Category> is found in current policy	Repeat until all categories have been asked
According to your knowledge, does your company have a policy that defines <information security object>"	Yes/No/Don't know	Yes if <Information security object> is found in current policy	Repeat until all objects have been asked

According to your knowledge, what does the policy say about <information security object>"	List all Object Content Templates for the Information security object.	The Object Content that is defined in the Policy for this Information security object	Repeat until all objects have been asked

For the general security knowledge part of Survey, the questions, answer options and right answers are managed by the Manager and Superuser in a way similar to the Policy Management.

A survey consists of a link to a policy, a number of questions, answer options, and indication of the right answer option together with a score for each option. Default score for the right answer is 10 and default score for wrong answers is 0.

Questions are stored in a table in the security object database.

The answers are stored in a table that links to the user, to the questions and to the survey. If user requested to be anonymous, the answers are added to answer consolidation tables that allow for the Result reports to be generated without saving individual user responses.

Using information security objects in information security learning

The ISO's are used as (part of) the content in security learning.

Effects: Users of the information learning system will be presented not only with general knowledge, but also with the specific content of the organisation they belong to.

Users will learn not only the general knowledge but will also learn what ISO's manager users have decided are relevant for the users to know in their organisation.

Using user definitions between policy, survey and education modules

The user settings and permissions that are defined in the management module are re-used in the policy, survey and the education modules.

Effects: Users can without the need for repeating authentication routines (e.g. passwords) be educated and surveyed in e.g. security policies, security instructions, security surveys, security learning.

Prior art

Security policy applied to common data security architecture, e.g. United States Patent Application 20010018746 which is an architecture for that allows users to generate trust policies independent of the computers they have the responsibility of managing.

Security management system and security managing method, e.g. United States Patent Application 20010023486, which is a database based security management and security audit system. This invention is about having users managing systems.

American vendors Pentasafe and Intellitactics' provide security policy management tools or services: One is a product named "Livingpolicy", another is "Vigilent Policy Manager". Both also provide simple surveying functions. Yes/No questionnaires that refer to security policy requirements are known prior to this invention.

Electronically performed surveys with functions that allows a manager type user, e.g. a security manager or e.g. an officer to put in free text style questions in a number of questionnaires to users are known.

E-learning systems and learning management systems are known. Security learning classes, also web based, are known. These classes target system administrators, or network administrators or security administrators, and do not target all relevant users in an organisation.

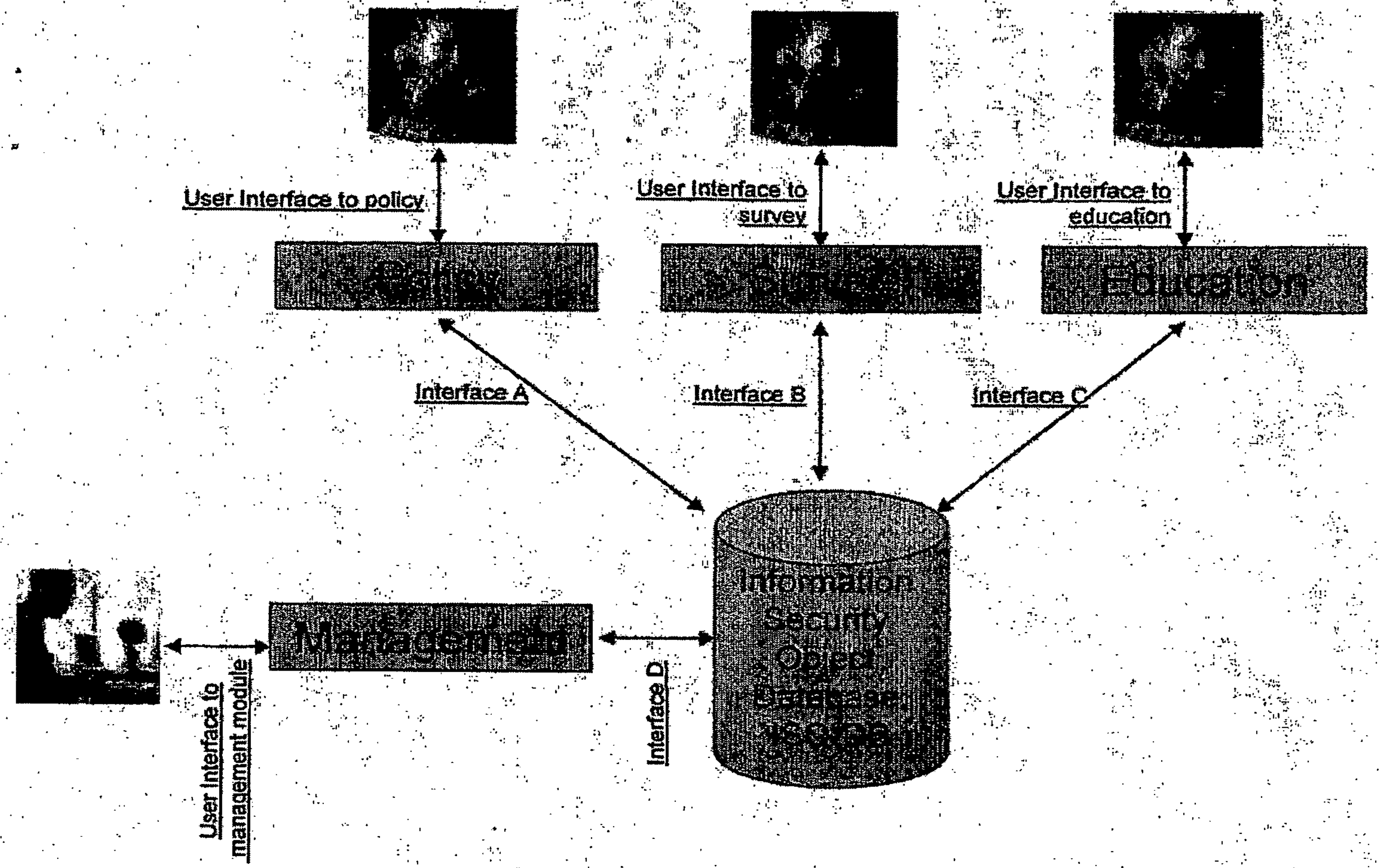
Definitions

In some organisations or contexts the terms "security instruction" "security rule", or "security procedure" are used instead or together with of the term "security policy".

Patent Claims

A method and a system as herein described and illustrated in the figures.

Fig. 1



User Interface to policy
User Interface to survey
User Interface to education
Policy
Survey
Education
Interface A
Interface B
Interface C
Information Security Object Database ISODB
Management
Interface D
User Interface to management module

Fig. 2

Security Policy Creation

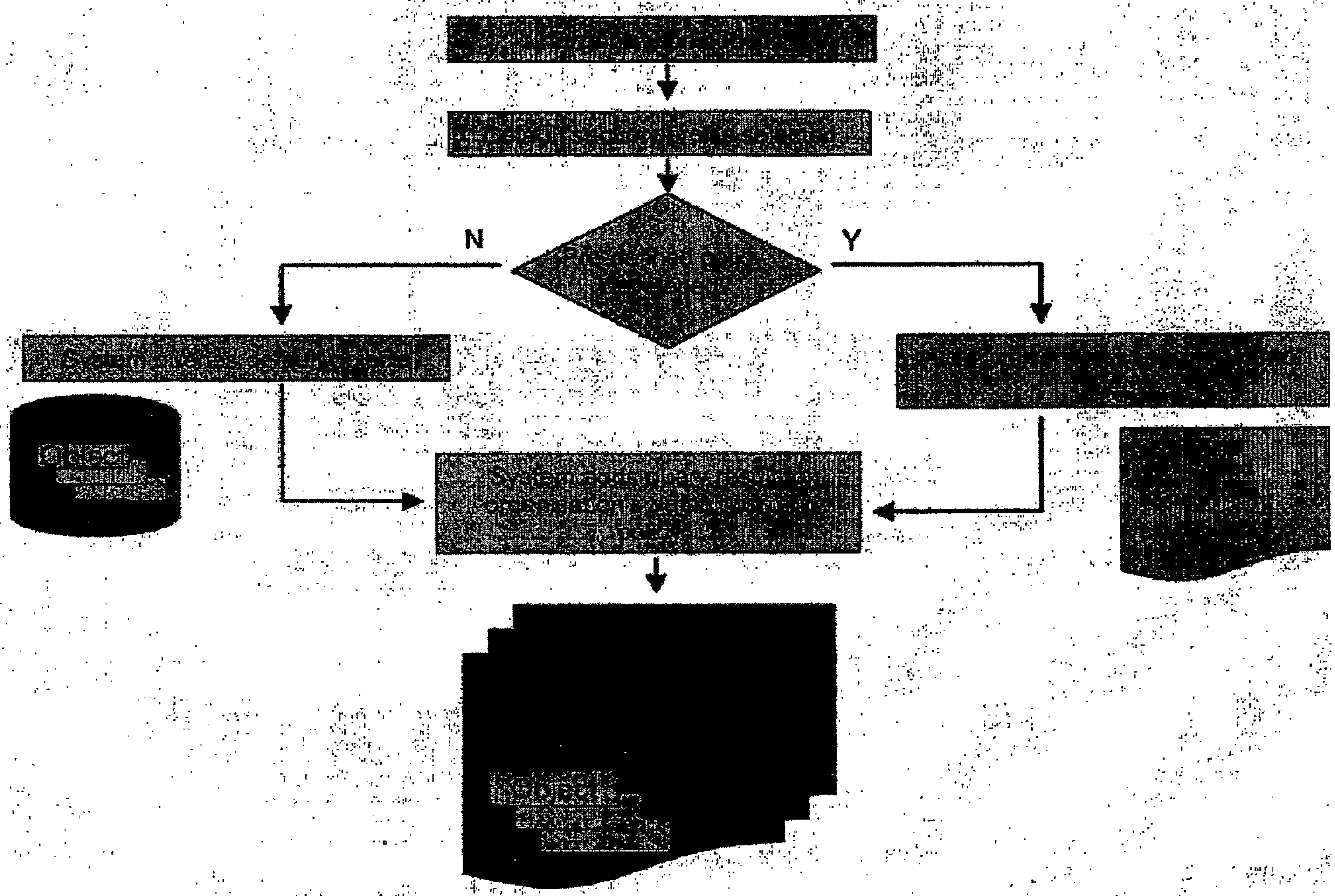
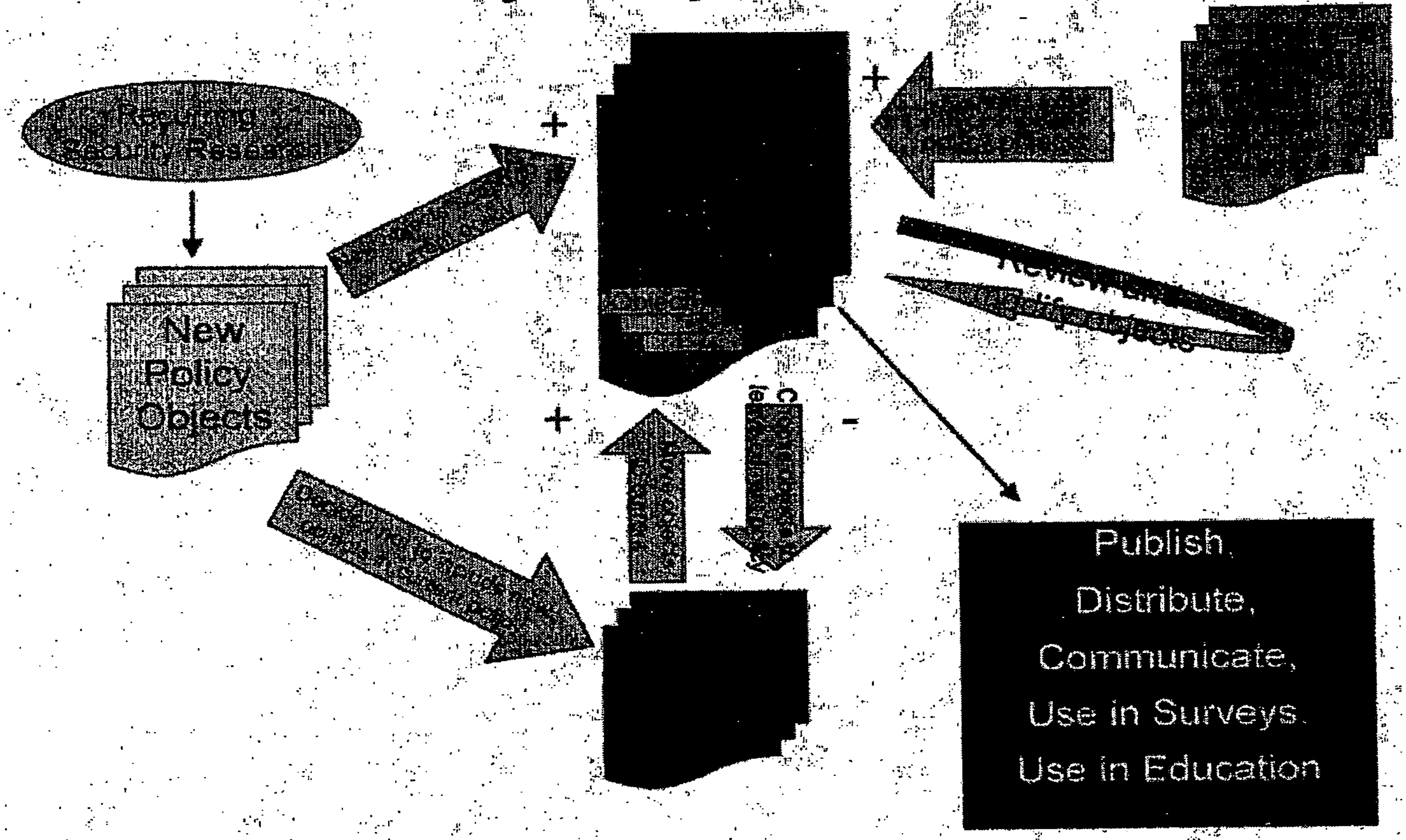


Fig. 3

Security Policy Management



Security Research

New Policy Objects

Review and modify objects

+

+

+

-

Publish,
Distribute,
Communicate,
Use in Surveys.
Use in Education